

ABSTRACT

METHOD FOR MAKING SECURE A SENSITIVE INFORMATION PROCESSING IN A MONOLITHIC SECURITY MODULE, AND ASSOCIATED SECURITY MODULE

The invention relates to a method for protecting the processing of sensitive information in a security module with a monolithic structure, the module comprising information processing means (9) and means for storing (3, 4) information capable of being processed by said processing means, characterized in that it comprises the following steps:

- selecting a piece of sensitive information in the storage means;
- determining (7) a specific condition for the integrity of said information;
- reading the information and transmitting (1) it to the processing means;
- verifying (11) during the processing of the information that the specific condition is satisfied;
- disabling the processing of the information if the specific condition is not satisfied.

The invention also relates to the associated security module.

Fig. 4